ISPP

Information Services Policy and Procedures

Effective Date: 01/14/2013

Policy: Password Management and Provisions

Where users belong to any Administered KDADS system, their password settings are to meet the following.

Passwords will be:

- Individually owned
- Kept confidential and not shared with other users
- Changed whenever disclosure has occurred or may have occurred
- Changed significantly (i.e., not a minor variation of the current password)
- Expires every sixty days
- When a password has been changed there is a three day waiting period before you can change it again
- A minimum of eight characters and contain at least one of each of the following: a number, an upper case letter, a lower case letters, and a special character

Passwords must not be:

- Repeated for at least six cycles of change or a year
- Repeating sequences of letters or numbers (e.g. rrr, 123123)
- Names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names)
- The same as the user id
- Words that can be found in a dictionary
- Displayed during the entry process
- Written down and displayed in an obvious place
- The same for all systems the user accesses
- Stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

Procedure:

1. **Establishing passwords.** New user accounts will have a standard ("default") password associated with them. Users will be prompted to change this right away at their first logon to any system. This is so someone else isn't able to use the default security code to masquerade KDOA users. Once established, the password is encrypted in the system - not even the Information Services Division can determine what user's passwords are. The Help Desk can set a new password up for users if forgotten.

2. **Make passwords difficult for someone to guess.** Guidelines for users to construct their own passwords.
   - Minimum eight characters long. (Enforced by the Network Operating System & Other Systems)
   - Include at least one numeric digit
   - Include at least one lower case letter
   - Include at least one upper case letter
   - Include at least on special character
   - No spaces

- No simple repetition of letters or numbers
- Is not the same as your user (logon) ID
- Does NOT include any "real world" information that someone else could use to guess a password (e.g., car license number, birth date, name of spouse/child/pet). It's a good idea to create "nonsense words" to remember passwords (examples: 2Tall4me, B92morZ, kiLrTm8o etc).

3. **Users should not reveal their passwords.** Users should not write it down on a Post-It note stuck on their computer monitor, or not tape it to the bottom of their telephone or keyboard. In other words, if it's convenient for users to check it, then it's also convenient for other KDADS employees, the evening cleaning crew, or anyone else who gains access to KDADS office space to find and use it. Similarly, users should not put their password into an online file. Users should not put it in any automated command scripts (typically used to speed up a login process).

4. **Change passwords regularly.** Users may never know if someone else has discovered their password. To limit the chances of someone gaining advantage with a user's password, the KDADS network prompts users to change their password every 60 days. If this isn't done within a five-login grace period, the password expires, and the user must contact the Help Desk to re-establish their account. E-mail and files will NOT be discarded if this happens. The new password should be quite different from the previous ones, rather than a variation. If a user forgets their password and unsuccessfully attempts to log into the network more than ten times, their account will also become locked and will remain locked for one hour until it automatically unlocks. If a user does not want to wait for the lockout duration to transpire they must contact the Help Desk to have the account unlocked. In all cases of password problems or questions, users are to contact the KDADS Help Desk for assistance.

5. **Beware of "social engineering" attacks.** Users should be especially wary of anyone who asks them for their password to "perform emergency system maintenance." This is a ruse frequently employed by malicious outsiders to gain access to a computer system. *Should users ever be requested to reveal their login user name, password, or network ("IP") address, they should notify the KDADS ISD Help Desk immediately, as someone may be trying to gain unauthorized entry to KDADS systems.*